Walking on APT31 infrastructure footprints

SEKOIA.IO's Cyber Threat Intelligence team had **an in-depth look at the APT31 intrusion set at the beginning of 2021** when the BfV (Bundesamt für Verfassungsschutz)[1] and McAfee[2] released some new information. A few months later, the French National Cybersecurity Agency (ANSSI) also released a short publication with several IoCs[3], showing that the intrusion set was still active and of concern as multiple national agencies had been involved.

All of these IoCs were mainly IP addresses, and **many of them seemed to be linked to SOHO routers**, mostly Pakedge routers at the time. With that observation, we investigated more deeply to see if we could find more infrastructure and implants used by this intrusion set.

A BRIEF ON THE APT31 CREATURE

APT31 (aka Zirconium or Judgment Panda) is an Advanced Persistent Threat group whose mission is likely to gather intelligence on behalf of the Chinese government. Similar to other nation-state actors, **the group is focusing on data of interest to the PRC** (People's Republic of China) and its strategic and geopolitical ambitions, rather than on specific verticals.

The Chinese adversaries are considered some of the most prolific state-sponsored cyber actors on the planet. According to Microsoft's observations, from July 2020 to June 2021, China-based threat actors displayed the strongest interest in targeting critical infrastructure among all the other nation-state threats[4].

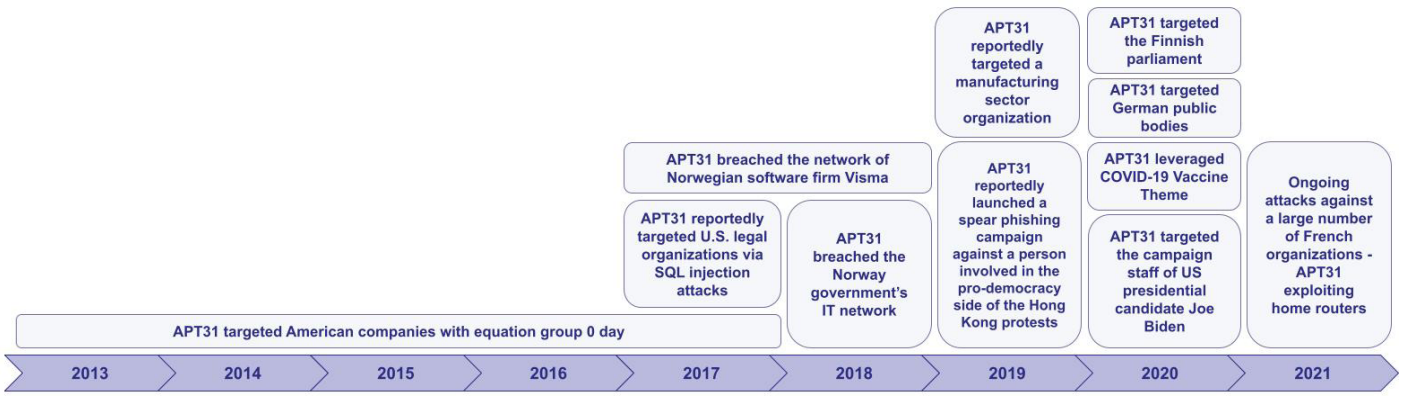

Figure 1. A timeline of the publicly reported APT31-related campaigns

As shown in Figure 1 and in alignment with available public reports, APT31 has been active since at least 2013 and its 2021 campaign targeting numerous French entities is still ongoing.

Even if the public literature on this intrusion set is quite limited, APT31 is known to use — among others vectors — spear phishing to get a foothold in the victims' networks. Although **their recent campaigns weren't technically sophisticated**, they succeeded in bypassing network defences by employing only legitimate websites and services to host their implants (GitHub) and interact with them once executed on the victims' workstation (use of DropBoxAPI)[5]. It has also been spotted targeting organizations via SQL injection attacks, as well as leveraging stolen credentials to gain initial access.

APT31 and other Chinese state–backed actors have been lately the object of several European governments' attribution statements.

Back in July 2021, the UK accused the Chinese Ministry of State Security (MSS) of supporting the APT31 group's activities[6]. At nearly the same time, the EU detected malicious cyber activities with significant effects that **targeted key European industries** and linked them to APT31[7]. In both cases, official statements mentioned APT31 alongside another Chinese attacker group — APT40.

Moreover, **authorities suspect APT31 to be a group of contractors working directly for China's MSS**, or even members of the People's Liberation Army (PLA) Strategic Support Force, as reported by other sources.

HUNTING IN THE APT31 INFRASTRUCTURE FOOTPRINTS

APT31 is one of the few intrusion sets known to have been seen compromising SOHO routers to compose its operational infrastructure, since at least November 2019, date on which a sample of the backdoor used on compromised routers was uploaded to VirusTotal for analysis (MD5: 77c73b8b1846652307862dd66ec09ebf). However, this implant can be much older as there is no compilation date associated with ELF files.

The Operational Relay Boxes (ORB) associated with this infrastructure are used as proxies for frontal attacks, active and passive reconnaissance and also as command and control servers for several implants. **Till today, we don't know how they compromised these routers.** It is likely that they used a mix of known and unknown vulnerabilities to achieve remote code execution in order to drop their implants and other redirector tools.

We found ways and heuristics to illuminate some parts of their infrastructure and track it over time. **The C2 domains used by this intrusion set have several characteristics** such as:

• Patterns: lots of domains had technical strings such as "update", "check", "cloud" or "service" along with some IOT/router's brands (Mikrotik, Netgear, Qnap, Nec).

• DNS configuration: most of them don't resolve anything without an appropriate subdomain such as "www", "api", "sso" etc.

• DNS providers: APT31 mainly uses four DNS providers: Monovm, Cloudflare, Topdns and most recently Hosteons, which we've seen used only for two domains so far.

• Fake registrant and associated email: the name is mostly composed like a real name (eg. Joseph Edwards) with an associated email address using protonmail.ch, email.cz, post.cz or inbox.lv.

• The resolution timeframe of these domains doesn't exceed a few days, which is also relevant from an analyst's point of view.

As the domains were resolving to SOHO routers, it was also possible to track them using this particularity. Indeed, **it is relatively rare that a domain from these DNS providers points to some domestic autonomous systems.**

On the other hand, the network appliances compromised by APT31 have technical characteristics (eg. administration panels, specific certificates or banners) allowing anybody to recover thousands of IP addresses using them. By using passive DNS resolutions on these IP addresses, it was possible to discover new C2s when an observed FQDN pointing to them had the previously mentioned characteristics.

Finally, **we discovered nearly 50 IP addresses and 34 domain names** following ANSSI's publication, with an overlap of one IP address resolved by the domain www.fwcheck[.]com. The table below summarises the brands of network appliances that composed the C2 infrastructure used by APT31 until July 2021.

The confidence value depends on the number of heuristics (explained above) that matched as well as on whether other sources already mentionned the C2 or not.

Brand seen on C2	Number of C2s	Confidence
Pakedge	41	High
CyberOAM	3	High
Netgear VPN firewall	2	Low
D-LINK	1	Low
Others	5	Low

Since July 2021, we have observed a shift in their infrastructure. **They left their historical "Pakedge infrastructure"** and moved it to new clusters composed this time of several other brands and nameservers in order to avoid infrastructure illumination by analysts.

Since then, it has become more difficult to follow their tracks although we can still see several new C2s such as neccloud[.]net — resolving to 5.252.176[.]102, a server under the MivoCloud umbrella — or netgearcloud[.]net, resolving to a domestic IP address based in Sweden on September 22, 2021.

We link these domains to APT31 with high confidence as they match most of the infrastructure heuristics established during the investigation.

However, it's worth noting that not all their Operational Relay Boxes are resolved by domains names. Thenceforth, the IoCs list provided at the end of this Brint is obviously non-exhaustive and **shows only a small fraction of their operational infrastructure** used for attacks in 2021.

IMPLANTS SEEN DURING THE WALK

By looking at the implants connecting to this infrastructure in open source, **we have been able to get several implants**, that we assess were used by APT31 during their operations, such as Cobalt Strike beacons and an ELF implant dubbed "unifi-video" (MD5: 4640805c362b1e5bee5312514dd0ab2b), impersonating a well known IOT brand.

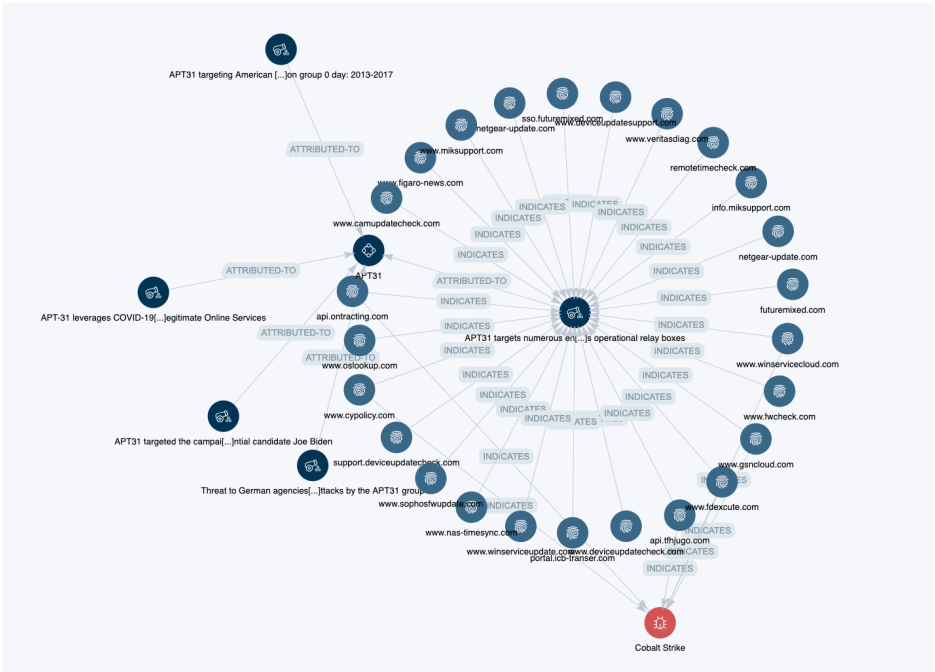

Figure 2. Links between some APT31 campaigns, indicators and malware/tools from SEKOIA.IO Intelligence Center.

Among standard red-teaming tools, **APT31 seems to be using Cobalt Strike as an n-stage implant** to persist inside the victim's network. As shown in the table below, several beacons connecting to the "Pakedge infrastructure" have been sent to VirusTotal packed in a PE to VirusTotal. It is worth noting that as they have been packed in an executable file, **the corresponding hash can't be used to hunt for APT31 in your network.**

Packed beacons MD5 hashes	Associated C2
f707759e05ab58296071ec50cc04c9fc	fdexcute[.]com
dc30a177a104717d652a49887851f033	api[.]ontracting[.]com
362057b23605d83130bdeac749d404f2	www[.]cypolicy[.]com
0d71876ba535cde68c21aa9b3bb063d1	www[.]winservicecloud[.]com

Last but not least, our Cobalt Strike trackers spotted two Cobalt Strike listeners on the discovered infrastructure:

Brand seen on C2	Number of C2s	Description
www[.]gsncloud[.]com	68.146.18[.]127	Cobalt Strike Malleable C2 Jquery profile from 22/03/2021 to 29/04/2021
api[.]tfhjugo[.]com	83.81.73[.]23	Cobalt Strike default headers on port 443 from 21/04/2021 to 17/05/2021

Unfortunately, the configurations associated with **the discovered Cobalt Strike beacons are pretty common** and prevented us from getting more discriminant indicators linked to their use of Cobalt Strike.

During the hunting, we found an ELF implant on VirusTotal[8] which matched the C2 — hardcoded in the sample — www[.]moperfectstore[.]com. **We attribute this domain with medium to high confidence to APT31** as it resolved to Pakedge and CyberOAM appliances and matches some domain heuristics described above. As the domain didn't have any existence prior to 2021, we assess with medium to high confidence that the implant was used by APT31.

This implant, dubbed "unifi-video" (MD5: 4640805c362b1e5bee5312514dd0ab2b), is a statically-linked stripped 64bits ELF. Unifi-video is a well known legitimate software that describes itself as a "Centralized management system for Ubiquiti UniFi surveillance cameras". It therefore echoes the compromised-appliance infrastructure used by APT31.

It turns out that this ELF is the Tiny SHell GitHub repo backdoor, thanks to Billy Leonard for pointing that out on Twitter. Tiny SHell has been used by multiple threat actors since several years now and it is not surprising to see APT31 using it. There is however no indication whether this Tiny SHell backdoor is used in the infrastructure or to persist in an appliance of a final victim, somewhere.

CONCLUSION

Despite the lack of open source literature on this intrusion set, **APT31 remains a prolific threat for years for many occidental entities working on government and strategic issues.** As of today, we don't have a clear view of what they are looking for once they compromised the networks if it is for pre-positioning or data theft.

This Brint aimed to disclose some of their operational infrastructure and tools used this year so that you can look for possible compromises in your networks.

If you are also investigating APT31, don't hesitate to share your thoughts with us at threatintel@sekoia.fr to better understand and track down their infrastructure.

EXTERNAL REFERENCES

[1] Bedrohung deutscher Stellen durch Cyberangriffe der Gruppierung APT31

[2] MVISION Insights: Potential APT31 Activity Against Political Targets,

[3] Campagne d'attaque du mode opératoire APT31 ciblant la France

[4] FY21 Microsoft Digital Defense Report

[5] APT-31 Leverages COVID-19 Vaccine Theme and Abuses Legitimate Online Services

[6] UK and allies hold Chinese state responsible for a pervasive pattern of hacking

[7] China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory

[8] Sample 4640805c362b1e5bee5312514dd0ab2b

[9] Linux.Rekoobe.1

[10] Linux Rekoobe Operating with New, Undetected Malware Samples

IOCS

The IOCs are provided “as is”. Even if the domain names are a reliable way to hunt APT31 in your network logs, the IP addresses can produce false positives as they rely mostly on legit home routers. All the IOCs can be downloaded in JSON STIX2.1 and CSV formats on the SEKOIA.IO Github: https://github.com/SEKOIA-IO/Community/tree/main/IOCs

TACTICS, TECHNIQUES AND PROCEDURES (TTPS)

Exploit Public-Facing Application (T1190)
Non-Application Layer Protocol (T1095)
Application Layer Protocol (T1071)
Process Injection (T1055)
Phishing (T1566)
Compromise Infrastructure (T1584)
Acquire Infrastructure (T1583)
Develop Capabilities: Malware (T1587.001)
Obtain Capabilities: Malware (T1588.001)

DOMAIN NAMES

netgearcloud[.]net
neccloud[.]net
netgear-update[.]com
www[.]netgearupdatecheck[.]com
ns[.]netgear-update[.]com
www[.]winserviceupdate[.]com
winserviceupdate[.]com
www[.]pi-hole[.]us
www[.]qnapphoto[.]com
update[.]hardis-software[.]com
www[.]moperfectstore[.]com
info[.]miksupport[.]com
api[.]ontracting[.]com
www[.]fwcheck[.]com
portal[.]icb-transer[.]com
www[.]cypolicy[.]com
remotetimecheck[.]com
api[.]tfhjugo[.]com
www[.]camupdatecheck[.]com
www[.]jsonamazon[.]com
www[.]serverupdatecheck[.]com
www[.]nas-timesync[.]com
www[.]mikupdate[.]com
www[.]mikrotikupdate[.]com
www[.]winservicecloud[.]com
www[.]sophosfwupdate[.]com
www[.]deviceupdatecheck[.]com
sso[.]futuremixed[.]com
futuremixed[.]com
support[.]deviceupdatecheck[.]com
www[.]figaro-news[.]com
www[.]switch-netgear[.]com
www[.]veritasdiag[.]com
fdexcute[.]com
www[.]fdexcute[.]com
www[.]miksupport[.]com
status[.]veritasdiag[.]com
www[.]deviceupdatesupport[.]com
www[.]keys-networks[.]com
srv[.]keys-networks[.]com
keys-networks[.]com
www[.]oslookup[.]com
www[.]gsncloud[.]com

IP ADDRESSES

213[.]21[.]100[.]188
108[.]46[.]133[.]103
108[.]54[.]184[.]30
116[.]86[.]137[.]232
158[.]174[.]170[.]19
184[.]75[.]129[.]113
185[.]129[.]252[.]187
185[.]130[.]165[.]59
185[.]89[.]55[.]24
185[.]96[.]198[.]75
188[.]165[.]73[.]52
189[.]121[.]150[.]254
213[.]238[.]234[.]249
217[.]210[.]180[.]113
217[.]211[.]53[.]251
45[.]147[.]229[.]194
50[.]71[.]100[.]164
58[.]182[.]61[.]137
58[.]96[.]237[.]98
71[.]64[.]151[.]132
73[.]229[.]137[.]54
78[.]82[.]247[.]37
81[.]227[.]88[.]108
81[.]232[.]51[.]161
81[.]234[.]227[.]62
81[.]236[.]182[.]199
81[.]83[.]4[.]48
82[.]127[.]26[.]151
82[.]136[.]76[.]142
83[.]253[.]189[.]234
83[.]81[.]73[.]23
84[.]23[.]132[.]127
85[.]166[.]160[.]50
85[.]226[.]191[.]68
85[.]229[.]70[.]242
86[.]4[.]247[.]233
88[.]129[.]239[.]96
88[.]129[.]39[.]248
88[.]88[.]141[.]177
89[.]31[.]225[.]131
89[.]31[.]228[.]228
89[.]31[.]228[.]238
90[.]224[.]137[.]58
91[.]117[.]133[.]53
91[.]235[.]247[.]248
93[.]240[.]145[.]166
95[.]236[.]16[.]215
95[.]34[.]0[.]182
96[.]89[.]114[.]192
98[.]128[.]185[.]162
99[.]252[.]170[.]14
68[.]146[.]18[.]127
5[.]252[.]176[.]102

YARA RULES

```
rule unk_apt31_tsh_2021 {
   meta:
      description = «Detect APT31-linked TSH sample. This rule is quite specific with the $s3 string. We
would advise removing this string to cover other TSH samples.»
      version = «1.0»
      creation_date = «2021-10-11»
      modification_date = «2021-10-11»
      classification = «TLP:WHITE»
      hash = «4640805c362b1e5bee5312514dd0ab2b»
      source=»SEKOIA.IO»
      version=»1.0»
   strings:
      $s1 = { C6 00 48 C6 40 05 49 C6
      40 01 49 C6 40 06 4C C6
      40 02 53 C6 40 07 45 C6
      40 03 54 C6 40 08 3D C6
      40 04 46 C6 40 09 00 }

      $s2 = { C6 00 54 C6 40 03 4D C6
      40 01 45 C6 40 04 3D }

      $s3 = «www.moperfectstore.com»
   condition:
      int32be(0) == 0x7f454c46 and
      filesize < 1MB and filesize > 900KB and
      all of them
}

rule apt_misp_apt31_orb_2021 {
   meta:
      description = «Detects APT31 ORB implant»
      version = «1.0»
      creation_date = «2021-10-11»
      modification_date = «2021-10-11»
      classification = «TLP:WHITE»
      hash = «77c73b8b1846652307862dd66ec09ebf»
            source=»SEKOIA.IO»
      version=»1.0»
   strings:
      $s1 = «mv -f %s %s ;chmod 777 %s»
      $s2 = «GET /plain HTTP/1.1»
      $s3 = «exc_cmd time out»
      $s4 = «exc_cmd pipe err»
      $s5 = { 2e 2f [1-10] 20 20 64 65 6c }

   condition:
      int32be(0) == 0x7f454c46 and
      filesize < 800KB and         filesize > 400KB and
      4 of ($s*)
}
```

Who we are

SEKOIA.IO is a European cybersecurity SAAS company, whose mission is to develop the best protection capabilities against cyber attacks. The company created in France provides modern technologies, proven in the field, to enable its major account customers and cybersecurity service providers to neutralize cyber threats before they have consequences.

+ 1 000 000
assets
protected worldwide

+ 2 000 000
IoCs usable
daily

+ 1 000 000 000
events
processed daily

In the core of the community since 2008

SEKOIA.IO was born from the experience gained in the field over many years within the main European security incident response teams. After the creation of CSIRT / CERT teams to respond to targeted attacks, their support and their tools, we now offer them through SEKOIA.IO the technology to enhance their expertise on a large scale and allow them to collaborate effectively, with SOC players and Cyber decision-makers.

Cyber Threat Intelligence Service

SEKOIA.IO's products are based on the knowledge of attackers, their tactics, their operating methods, their tools and their infrastructures. All of this intelligence is produced by one of the largest private cyber threat intelligence service in Europe.

A Collaborative Approach

More than a company, SEKOIA.IO is a place of confrontation with new forms of threats. SEKOIA.IO advocates its European roots as well as the strength of the collective to protect and stay in the race against cybercriminals.

EU compliance

SEKOIA.IO designs and produces its cybersecurity solutions in France. All data is hosted in France and we are committed to applying European data protection rules (GDPR).

NEUTRALIZE THREATS BEFORE THEY DO

SEKOIA.IO

www.sekoia.io

Follow our news